REMARKS

Claims 1-18 were presented for examination. Claims 1-18 stand rejected in the Office Action dated June 23, 2010 (herein, "OA"). Claims 1, 3-5, 8-13 and 15-18 are amended herein. Claim 2 is canceled herein and new claims 19 and 20 are added herein.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. Specifically, the OA alleges that the specification does not provide antecedent basis for "personal digital key hard drive" as recited in claim 8, "reader/decoder circuit card" as recited in claim 9 and "identification data separately provided" as recited by claim 16.

Various portions of the specification provide antecedent basis for "personal digital key hard drive," as claimed. For example, page 3, lines 4-8 of the specification provides:

> As used herein, "PDK Key or Key" refers to a PDK-compliant wireless key providing access to PDK-protected objects. The acronym "PDK" refers to "personal digital key."
>
> A "PDK-hard drive" refers to a physical or "electronic" hard drive containing an integrated RDC.

Page 28, lines 27-28 of the specification also provides:

> securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the

Thus, "personal digital key hard drive" as recited in claim 8, is supported throughout the specification.

Claim 9 is amended herein to recite "a computer including a hard drive and wherein the reader/decoder circuit comprises a circuit board coupled to the hard drive." Support for this amendment is found throughout the specification. For example, page 31, lines25-27 provide:

> For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

Hence, the specification provides antecedent basis for claim 9.

Claim 16 is amended herein to remove the claim element "identification data separately provided" and to now recite:

> receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider;
> accessing the account associated with the user in the secure account database based on the activation code received from the personal digital key; and
> responsive to the activation code received form the personal digital key matching a subset of the user-specific data in the account associated with the user, authenticating the user to access content from the content provider.

Support for the amendments to claim 16 is found throughout the specification, for example at Figure 1; page 9, line 24 to page 10, line 25 and page 10, line 29 to page 11, line 26. Accordingly, the basis for the objection to claim 16 is now obviated.

Response to Rejections Under 35 U.S.C. § 101

Claims 1, 5 and 16-18 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. This rejection is overcome in view of the amended claims.

Claim 1 is amended herein to now recite "a tangible personal digital key," "a first wireless transceiver and "a second wireless transceiver." Support for this amendment is

found throughout the specification, for example page 9, line 24 to page 10, line 2; FIG. 4; page 14, lines 10-27 and page 33, line 30 to page 34, line 7. Accordingly, amended claim 1 now recites statutory subject matter. As claim 5 depends from claim 1, claim 5 now also recites statutory subject matter. Thus, reconsideration and withdrawal of the rejection of claims 1 and 5 is respectfully requested.

Claim 16 is amended herein to now recite "storing an account associated with a user in a secure user account database, the account including user-specific data and the account database included in a key provider" and "receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider." Thus, claim 16 now ties steps of the claimed method to an apparatus for performing the claimed method steps as suggested on page 4 of the OA. Hence, claim 16 now more clearly recites statutory subject matter, so reconsideration and withdrawal of its rejection is respectfully requested. As claims 17 and 18 depend from claim 16, claims 17 and 18 now also more clearly recite statutory subject matter, so reconsideration and withdrawal of their rejection is also respectfully requested.

Response to Rejections Under 35 U.S.C. § 112, 2nd Paragraph

Claims 2-4 and 7-18 are rejected under 35 U.S.C § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The OA alleges that it is unclear whether the "/" included in the "reader/decoder" circuit recited by claims 2-4 and 7-15 represents "or or and." Claim 2 is canceled,

thereby obviating the basis for its rejection. However, MPEP § 2173.01 recites in part that:

> A fundamental principle contained in 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers. They can define in the claims what they regard as their invention essentially in whatever terms they choose so long as **>any special meaning assigned to a term is clearly set forth in the specification. See MPEP § 2111.01.< Applicant may use functional language, alternative expressions, negative limitations, or any style of expression or format of claim which makes clear the boundaries of the subject matter for which protection is sought. As noted by the court in *In re Swinehart*, 439 F.2d 210, 160 USPQ 226 (CCPA 1971), a claim may not be rejected solely because of the type of language used to define the subject matter for which patent protection is sought.

Thus, provided the specification clearly defines terms used in the claims, applicants are permitted to "define in the claims what they regard as their invention essentially in whatever terms they choose." Multiple portions of the specification clearly describe a "reader/decoder circuit." For example, lines 13-15 of page 5 of the specification provide:

> An "RDC" refers to a Reader/Decoder circuit installed in a user's computer, or built into computer hard drive, or point-of-sale (POS) credit card swipe unit which communicates with PDK keys and decodes PDK data.

Additionally, the abbreviation "RDC" is used throughout the specification, as described above, to identify a "reader/decoder circuit." Accordingly, the claim element "reader/decoder circuit" is clearly defined by the specification and consistently used throughout the specification as a "RDC" or "Reader/Decoder circuit." Because the specification clearly defines "reader/decoder circuit," claims 3-5 particularly point out and distinctly claim the subject matter regarded as the invention. Accordingly, reconsideration and withdrawal of the rejection of claims 3-5 is respectfully requested.

The OA alleges that claims 8 and 9 recite terms that are not defined in the specification and "are not clear to one of ordinary skill in the art." *See* OA, page 5. Specifically, it is alleged that "a personal digital key hard drive" recited by claim 8 and "a reader/decoder circuit card" recited by claim 9 are not defined in the specification. As amended, claim 8 recites "a personal digital key (PDK)-hard drive," which is defined throughout the specification. For example, page 3, lines 4-8 of the specification provide:

> As used herein, "PDK Key or Key" refers to a PDK-compliant wireless key providing access to PDK-protected objects. The acronym "PDK" refers to "personal digital key."
>
> A "PDK-hard drive" refers to a physical or "electronic" hard drive containing an integrated RDC.

Page 28, lines 27-28 of the specification also provides:

> securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the

Claim 9 is amended herein to recite "a computer including a hard drive and wherein the reader/decoder circuit comprises a circuit board coupled to the hard drive." Support for this amendment is found throughout the specification. For example, page 31, lines 25-27 provide:

> For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

Thus, claims 8 and 9, as amended, particularly point out and distinctly claim the subject matter regarded as the invention, so reconsideration and withdrawal of their rejection is respectfully requested.

Claim 10 is amended herein to now recite "the wireless network is a secure radio frequency (RF) link between the computer and the personal digital key." Support for this

amendment is found throughout the specification. For example, page 6, lines 8-9 of the specification provides:

> In another embodiment, illustrated at 2000 in FIG. 17, the PDK 1010 interfaces with a computer 2002 through a secure RF link 2004. The

Thus, amended claim 10 particularly points out and distinctly claims the subject matter regarded as the invention, so reconsideration and withdrawal of its rejection is respectfully requested.

Claim 16 is amended herein to now recite "storing an account associated with a user in a secure user account database, the account including user-specific data and the account database included in a key provider" and "receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider." Thus, amended claim 16 does not have a gap between the steps of the claimed method, as indicated on page 6 of the OA. Accordingly, reconsideration and withdrawal of the rejection of claim 16, and its dependent claims 17 and 18, is respectfully requested.

Response to Rejection to Claims Under 35 U.S.C. § 102

Claims 1, 2, 4, 6, 14 and 15 are rejected under 35 U.S.C. § 102(b) as being anticipated by US Patent Application No. 2002/0083318 ("Larose"). This rejection is overcome in view of the amended claims.

As amended, claim 1 now recites:

> a tangible personal digital key including a first wireless transceiver;
> a device coupled to the personal digital key via a wireless network, the device including a second wireless transceiver that receives data from the personal digital key and a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider, the device receiving data

from the provider and authenticating the data received from the personal digital key.

The claimed invention recites a system comprising a tangible personal digital key and a device coupled to the personal digital key through a wireless network. The tangible personal digital key includes a first wireless transceiver while the device includes a second wireless transceiver that receives data from the personal digital key. A reader/decoder circuit included in the device transmits the data received from the personal digital key to a provider and the device receives data from the provider authenticating the data received from the personal digital key. Support for the amendments to claim 1 is found throughout the specification, for example at page 11, lines 7-22 and at page 9, lines 7-16. Communication of data from the tangible personal key from the device to a provider beneficially allows more flexible assignment, distribution and use of personal digital keys.

Larose fails to disclose at least the claimed elements of "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider" and "the device receiving data from the provider and authenticating the data received from the personal digital key." Rather, Larose discloses integrating security functions into a digital appliance, such as a personal computer, to implement a computer software application using a trusted secure hardware adjunct to permit execution. Larose, ¶ [0008]. As disclosed by Larose, a secure hardware adjunct is a device that communicates with a digital appliance and also is capable of "storing secret data such as cryptographic keys and executing hidden software algorithms, and of performing cryptographic and other operations in a fashion at least partially controllable by the digital appliance." Larose, ¶ [0025].

Page 10 of the OA alleges that Figure 4 and paragraphs [0027], [0033], [0050] and [0070] of Larose disclose a computer transmitting and receiving data from a provider through an Internet connection. However, these cited portions of Larose, and the remaining disclosure of Larose, fail to disclose "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," as claimed. Figure 4 of Larose merely provides a high-level block diagram of a personal computer 400 connected to an internet server 440. However, in describing operation of the system shown by Figure 4, paragraphs [0072] and [0073] of Larose provide:

> [**0072**] At step **505**, the user invokes integration framework software **420** which then checks the ports of personal computer **400** for card reader **435**. At step **510**, integration framework software **420** displays a message asking the user to insert smart card **430** into card reader **435**. At step **515**, integration framework software **420** verifies the integrity of smart card **430**. More specifically, by interacting with smart card **430**, integration framework software **420** establishes, not only that it is a legitimate smart card with a known root of trust, but that it has appropriate programming (and optionally, appropriate stored rights and upload capability) to support the integration process and required hidden transformation for the computer software application to be processed.
>
> [**0073**] At step **520**, integration framework software **420** determines location of application neutral form **445** and sensitive functions **450**. At step **525**, the sensitive functions **450** and application neutral form **445** are downloaded from Internet server **440**.

Thus, Figure 4 of Larose and its associated description merely disclose using integration framework software operating on the personal computer to verify the integrity of a smart card. Data from the smart card is not transmitted to a provider in Larose, but integration framework software included on the personal computer itself establishes the legitimacy of the smart card. While the claimed invention recites a device including "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," Larose discloses integration framework software that retrieves an

application neutral form and sensitive functions from an Internet server to the personal computer after verifying a smart card.

Paragraphs [0027] and [0033] of Larose disclose:

> **[0027]** The secure hardware adjunct **12** may also have the capability to retrieve data from an Internet server that will be bound to the application executable form **24**. For example, this data could be a unique serial number for each use of the product and would allow per-use tracking. Such capability does not require any direct connections from the secure hardware adjunct **12** to the Internet server. As described earlier in the context of a Virtual Private Network application of smart cards, the cryptographic capabilities of the secure hardware adjunct **12** enable it to have a secure interaction with an Internet server even if the communication path goes through, for example, processor **16** of digital appliance **10**. The secure hardware adjunct **12** could also request user input to be incorporated into the application executable form **24**, such as a user name and password, to ensure that the user had the right to use the program.

> **[0033]** Sensitive functions **18** (or a subset thereof), such as digital rights management algorithms, are integrated with the application neutral form **20** by the secure hardware adjunct **12**. Sensitive functions **18** typically perform functions associated with digital rights management that are usually not specific to any given application package. Examples include algorithms designed to ensure that the computer software application cannot be executed on a machine other than a particular digital appliance **10**, with or without secure hardware adjunct **12**. However, the scope of sensitive functions **18** is not limited to digital rights management application. Other examples of sensitive functions **18** include interacting with an Internet server in order to authenticate a user; scanning a user's digital appliance to determine if the user has established a contract with the application publisher; requesting and downloading cryptographic keys from an Internet server; and scanning a digital appliance for identifying serial numbers or other appliance-specific identifiers.

While the claimed invention recites a device including "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," paragraph [0027] of Larose merely discloses that the secure hardware adjunct may be able to receive data from an Internet server without disclosing a reader/decoder circuit

included in the device transmitting "data received from the tangible personal digital key to a provider." Paragraph [0033] of Larose merely provides examples of sensitive functions enabled by the secure hardware adjunct and makes no disclosure of transmitting "data received from the tangible personal digital key to a provider," as claimed.

Paragraphs [0050] and [0070] of Larose disclose:

> **[0050]** Appropriate integration framework software **14** for the application neutral form **20** and sensitive functions **18** would then be selected. The above three software items would then be delivered to a user by CD-ROM, Internet download or any other means. One of more of these three software items could be delivered to a user separately and at different times. Upon delivery to the user, the integration and transformation steps of the present invention can be performed with the aim of producing an executable instance of the application neutral form **20** incorporating the desired sensitive functions **18** chosen by the integration framework software **14** based on factors including the environmental data **22**.

> **[0070]** An Internet server **440** hosts the sensitive functions **450** and the application neutral form **445** that are downloaded over the Internet to the personal computer **440** by means of the network interface or modem **425**. Integration framework software **420** is stored on hard drive **415**. Environmental data **465** is optionally used by integration framework software **420** and smart card **430**.

Rather than disclose "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," as claimed. Paragraph [0050] of Larose discloses that sensitive functions may be delivered via an Internet download. Paragraph [0050] of Larose and makes no disclosure of transmitting data received from the tangible personal digital key to a provider. Similarly, paragraph [0070] of Larose merely discloses that sensitive functions may be downloaded from an Internet server to a

personal computer. Hence, like the remainder of Larose, paragraphs [0050] and [0070] of Larose fail to disclose "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," as claimed.

Additionally, amended claim 1 recites "the device receiving data from the provider and authenticating the data received from the personal digital key," which is also not disclosed by Larose. At most, Larose discloses integration framework software residing on a personal computer that verifies the integrity of a smart card, or other secure hardware adjunct coupled to the personal computer. If the integration framework software establishes the legitimacy of the smart card, the integration framework software subsequently obtains an application neutral form and sensitive functions. Larose, ¶ [0072], [0073]. Thus, Larose does not receive data from a provider, as claimed, but merely discloses a device that locally determines the integrity of a smart card and subsequently retrieves information if the smart card is determined to be valid.

Thus, Larose fails to disclose each and every element of amended claim 1. Accordingly, claim 1 is patentably distinct from Larose and reconsideration and withdrawal of its rejection is respectfully requested. As claims 4, 6, 14 and 15 depend from claim 1, these dependent claims incorporate the elements of claim 1 and are also patentably distinct from Larose for at least the reasons presented above with respect to claim 1. Hence, reconsideration and withdrawal of the rejection of claims 4, 6, 14 and 15 is also respectfully requested.

Additionally, amended claim 1 is not obvious in view of Larose. While the claimed invention recites a device including "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," Larose merely discloses a

secure hardware adjunct that may be able to receive data from an Internet server after a device to which the secure hardware adjunct is connected locally verifies the integrity of the secure hardware adjunct. Larose, ¶ [0027]. In contrast to the claimed invention, Larose uses integration framework software operating on a personal computer to verify the integrity of a smart card coupled to the personal computer. No portion of Larose discloses or suggests transmitting data from the smart card. While the claimed invention transmits data received from a tangible personal digital key to a provider, Larose establishes the legitimacy of the smart card using integration framework software included on the personal computer and subsequently retrieves data from, rather than transmit data to, an Internet server to the personal computer. Larose, ¶ [0072], [0073]. As Larose merely discloses local authentication of a secure hardware adjunct using integration framework software rather than "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," Larose also does not suggest amended claim 1.

Hence, as Larose does not disclose or suggest at least the claimed element of "a reader/decoder circuit that transmits data received from the tangible personal digital key to a provider," claim 1 is patentably distinct from Larose. As claims 4, 6, 14 and 15 depend from claim 1, these dependent claims incorporate the elements of claim 1, so they are also not disclosed or suggested by Larose for at least the reasons presented above with respect to claim 1.

Claim 2 is canceled herein, thereby obviating the basis for its rejection.

Response to Rejections Under 35 U.S.C. § 103

Claims 3, 5, 7-13 and 16-18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent Application No. 2002/0083318 ("Larose").

As claims 3, 5 and 7-13 variously depend from claim 1, all elements recited by amended claim 1 are incorporated into claims 3, 5 and 7-13. Thus, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 3, 5 and 7-13. Accordingly, claims 3, 5 and 7-13 are also patentably distinct from Larose, so reconsideration and withdrawal of their rejection is respectfully requested.

As amended, independent claim 16 recites:

> storing an account associated with a user in a secure user account database, the account including user-specific data and the account database included in a key provider;
> providing a tangible, personal digital key to a user, wherein the personal digital key stores information unique to the user;
> receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider;
> accessing the account associated with the user in the secure account database based on the activation code received from the personal digital key; and
> responsive to the activation code received form the personal digital key matching a subset of the user-specific data in the account associated with the user, authenticating the user to access content from the content provider.

The claimed invention recites a method for securing computer readable media from unauthorized access by storing an account including user-specific data in a secure user account database and providing to the user a tangible personal digital key storing information unique to the user. A request to verify an activation code received from the personal digital key by a content provider is received and the account associated with the

user in the secure account database is accessed based on the activation code received from the personal digital key. Responsive to the activation code received from the personal digital key matching a subset of the user-specific data in the account associated with the user, the user is authenticated to access content form the content provider. Support for the amendments to claim 16 is found throughout the specification, for example at Figure 1; page 9, line 24 to page 10, line 25 and page 10, line 29 to page 11, line 26. The claimed beneficially simplifies authentication of a user to access content from a content provider.

Larose fails to disclose at least the element of "receiving, at the key provider, a request to verify an activation code received from the personal digital key by a content provider," as recited by amended claim 16. Rather, Larose discloses a secure hardware adjunct communicating with a digital appliance to prevent unauthorized use of computer software. Larose, ¶ [0001], [0005], [0025], [0026]. To authorize use of computer software, Larose discloses integration framework software stored in the digital appliance that verifies the integrity of the secure digital appliance. Larose, ¶ [0072]. As the digital appliance locally verifies the secure digital appliance, there is no disclosure in Larose of "receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider," as claimed. In Larose, there is no disclosure, or suggestion, of a request to verify an activation code that a content provider received from the personal digital key at the key provider. Rather, Larose merely discloses that a single entity, the integration framework software, authenticates a secure digital appliance. Nowhere does Larose disclose or suggest a key

provider receiving "a request to verify an activation code received from the personal digital key by a content provider," as claimed.

Thus, Larose does not disclose or suggest at least "receiving, at the key provider, a request from a content provider to verify an activation code received from the personal digital key by the content provider," as recited by amended claim 16. Accordingly, claim 16, as amended, is patentably distinct from Larose, so reconsideration and withdrawal of its rejection is respectfully requested.

As claims 17 and 18 depend from claim 16, all arguments advanced above with respect to claim 16 are also applicable to claims 17 and 18. Thus, dependent claims 17 and 18 are also patentably distinct from Larose, so reconsideration and withdrawal of their rejection is respectfully requested.

New Claims

New claims 19 and 20 are added herein and recite additional patentable elements, such as "identifying an account record associated with the user stored in a provider database using the account number" and "responsive to the data from the tangible personal digital key matching data included in the identified account record, completing a transaction for purchasing the product." Support for new claims 19 and 20 is found throughout the specification, for example page 8, line 25 to page 9, line 16.

CONCLUSION

Allowance of all claims is respectfully requested. The Examiner is invited to contact the undersigned at the number indicated below if the Examiner believes that direct contact will advance the prosecution of this case.

Respectfully submitted,
JOHN GIOBBI

Dated: September 22, 2010 /Brian G. Brannon/

Brian G. Brannon
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net